

SC-900T00-A Module 1: Describe the Concepts of Security, Compliance, and Identity



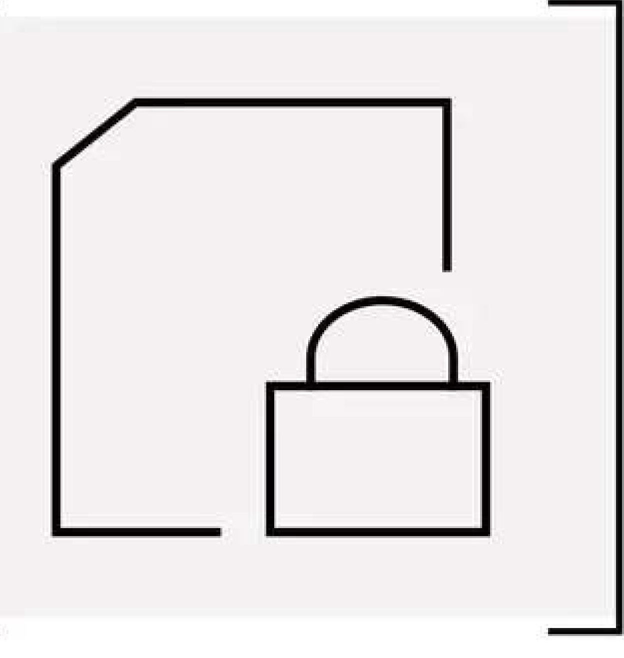


Describe security and compliance concepts and methodologies



Describe identity concepts

Lesson 1: Describe security and compliance concepts and methodologies



Lesson 1 Introduction

After completing this lesson, you'll be able to:

- Describe the Zero Trust and shared responsibility models.
- Describe common security threats and ways to protect through the defense in-depth security model.
- Describe the concepts of encryption and hashing.
- Describe the cloud adoption framework.

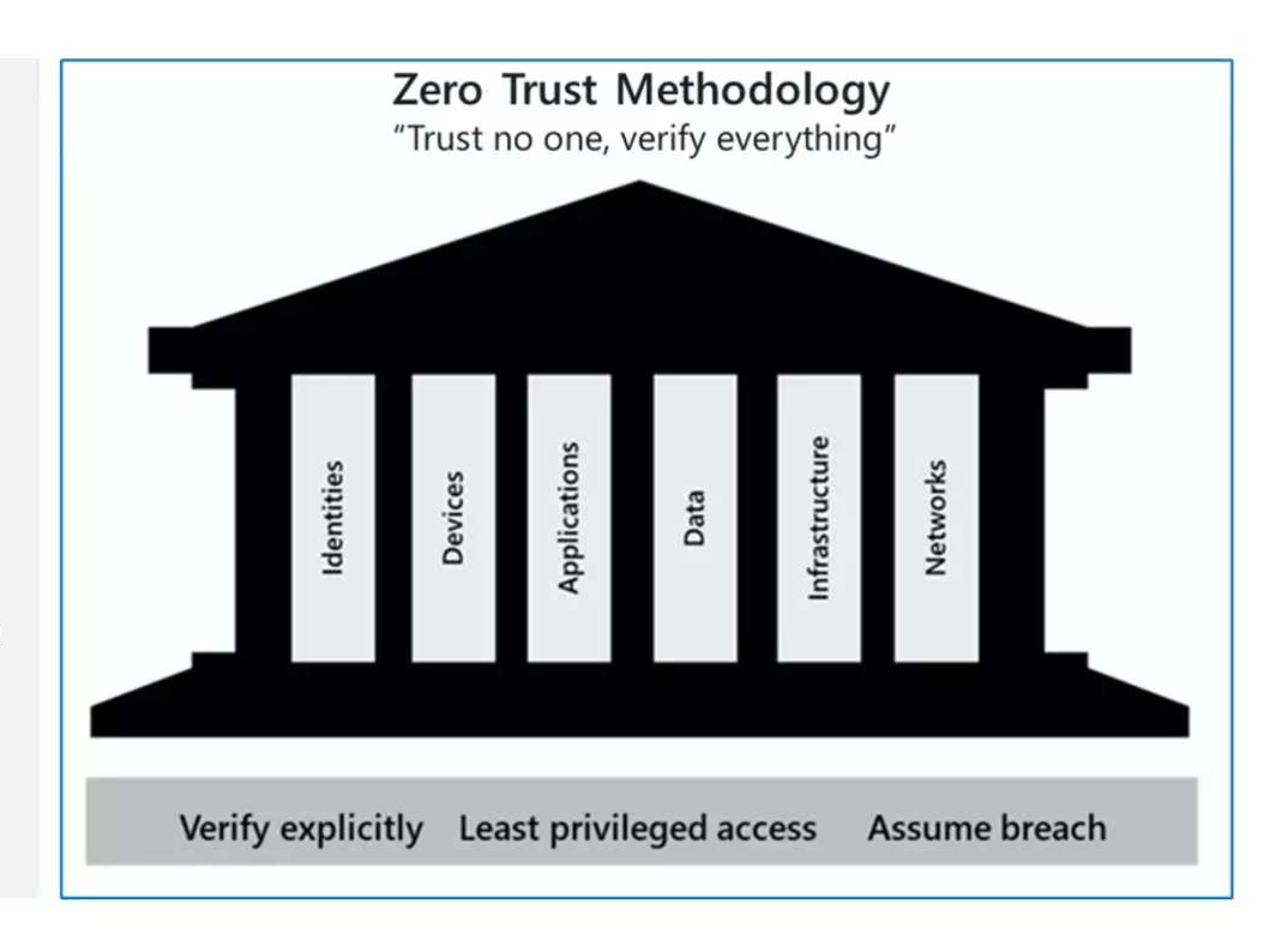
Zero-trust methodology

Zero Trust guiding principles

- Verify explicitly
- Least privileged access
- Assume breach

Six foundational pillars

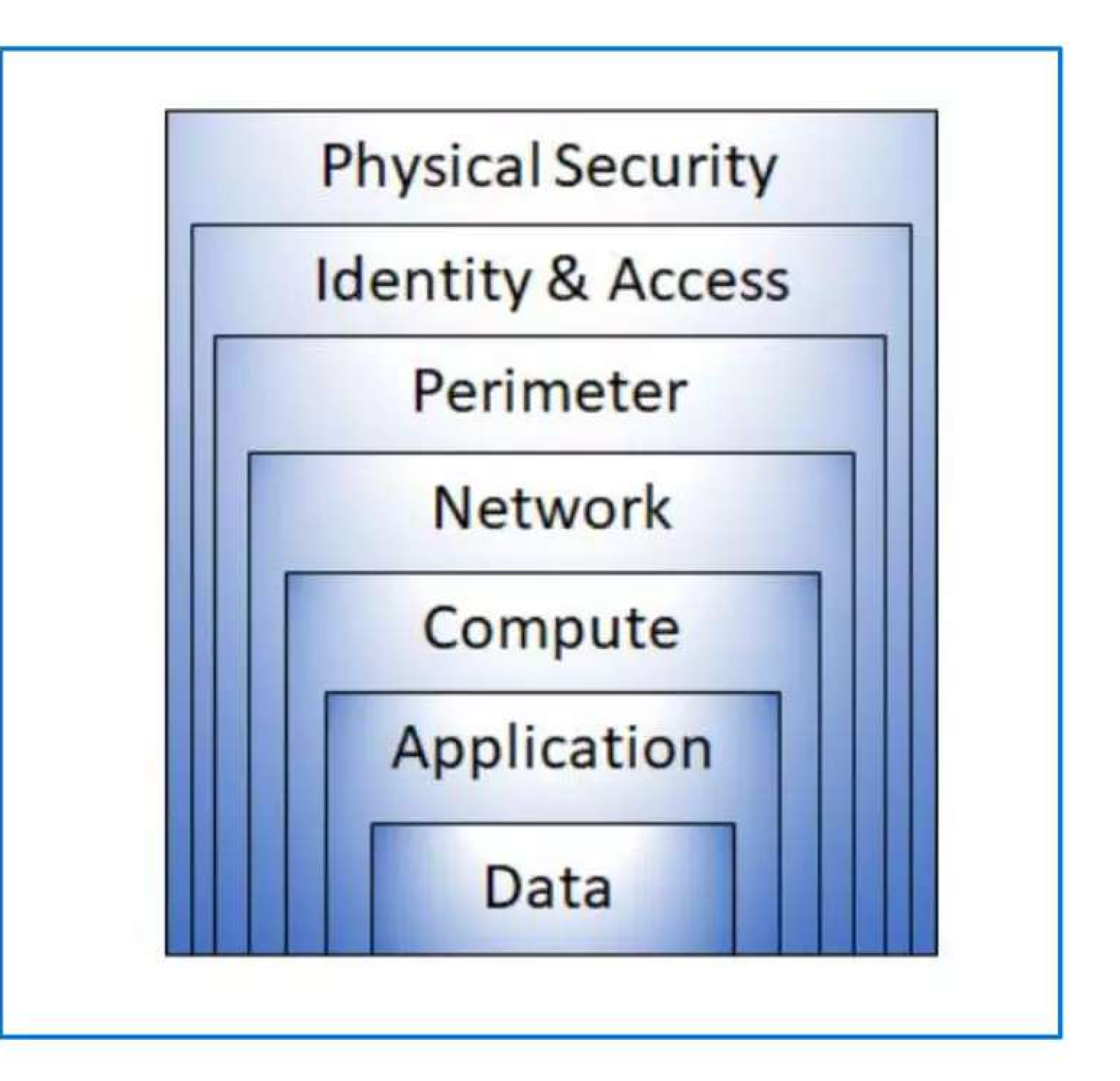
- **Identities** may be users, services, or devices.
- **Devices** create a large attack surface as data flows.
- **Applications** are the way that data is consumed.
- **Data** should be classified, labeled, and encrypted based on its attributes.
- **Infrastructure** whether on-premises or cloud based, represents a threat vector.
- **Networks** should be segmented.



Defense in depth

Defense in depth uses a layered approach to security:

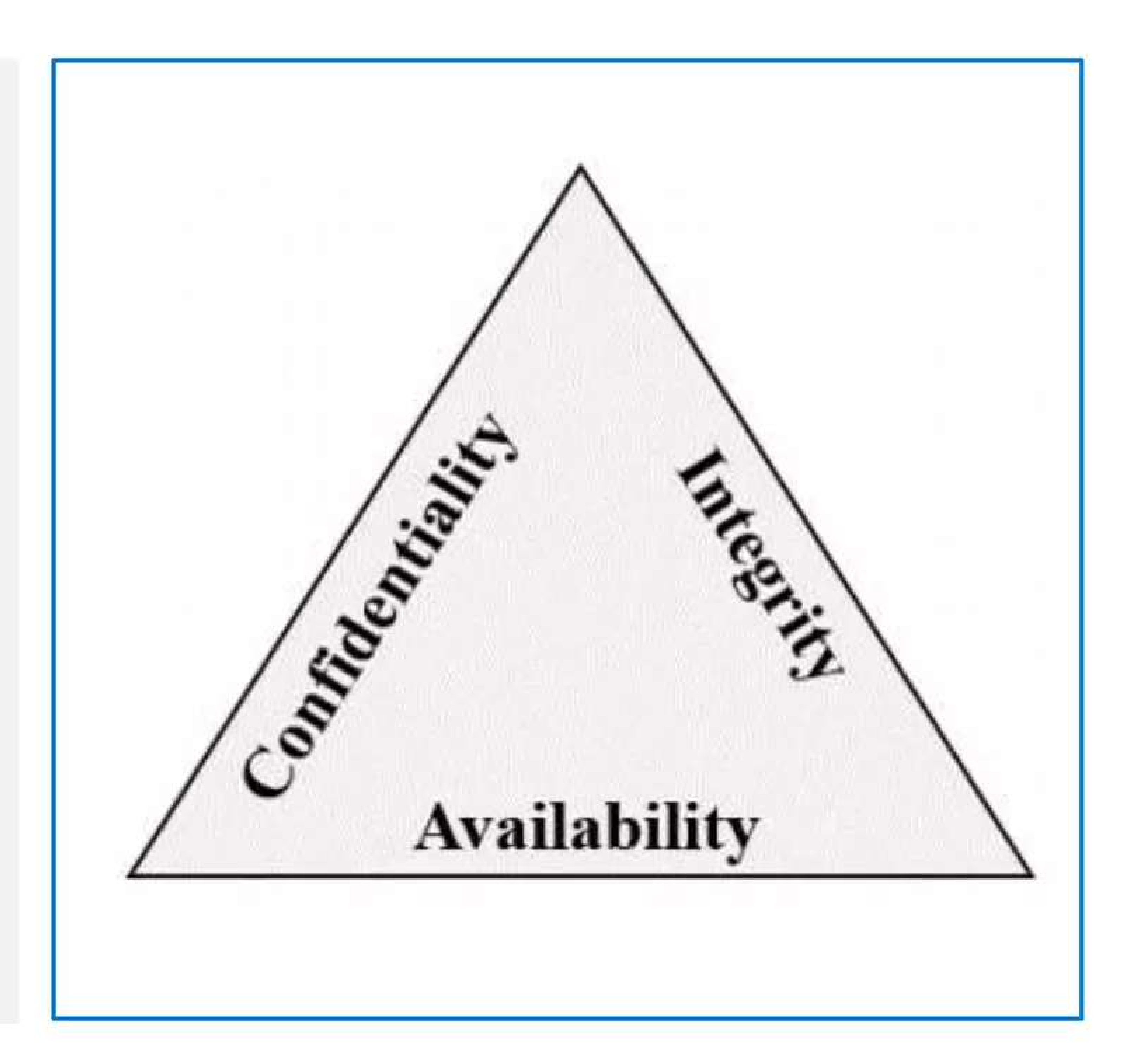
- **Physical** security such as limiting access to a datacenter to only authorized personnel.
- **Identity and access** security controlling access to infrastructure and change control.
- **Perimeter** security including distributed denial of service (DDoS) protection to filter large-scale attacks before they can cause a denial of service for users.
- **Network** security can limit communication between resources using segmentation and access controls.
- The **compute** layer can secure access to virtual machines either on-premises or in the cloud by closing certain ports.
- **Application** layer security ensures that applications are secure and free of security vulnerabilities.
- **Data** layer security controls access to business and customer data, and encryption to protect data.



Confidentiality, Integrity, Availability (CIA)

CIA - A way to think about security trade-offs.

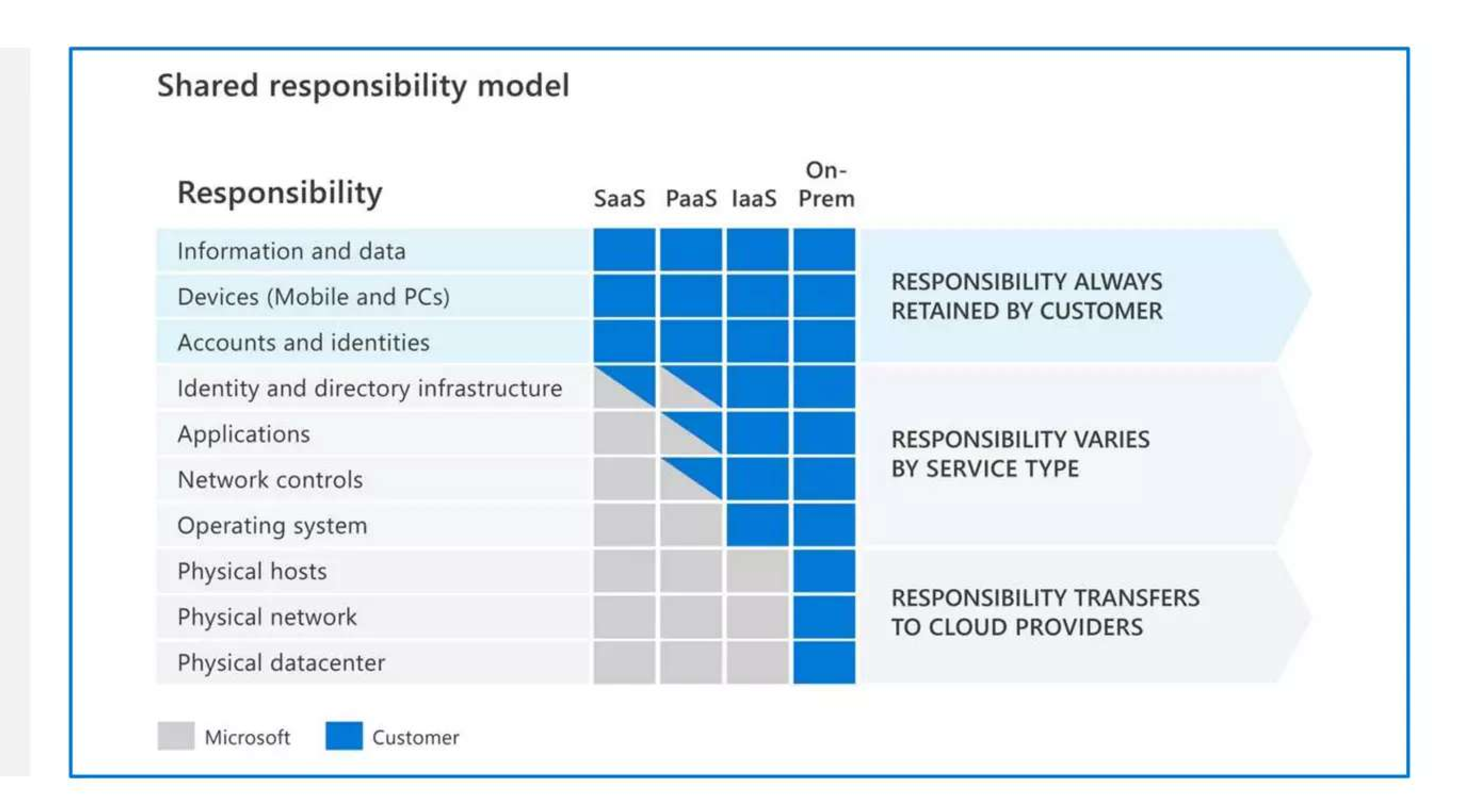
- **Confidentiality** refers to the need to keep confidential sensitive data such as customer information, passwords, or financial data.
- **Integrity** refers to keeping data or messages correct.
- **Availability** refers to making data available to those who need it.



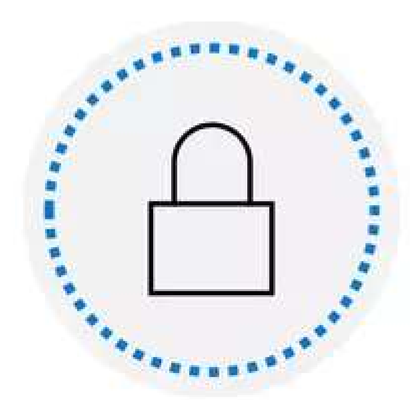
The shared responsibility model

The responsibilities vary based on where the workload is hosted:

- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)
- On-premises datacenter (On-prem)



Common threats



Data breach

Include:

- Tech support scams
- SQL injection
- Malware designed to steal passwords or bank details.
- Phishing

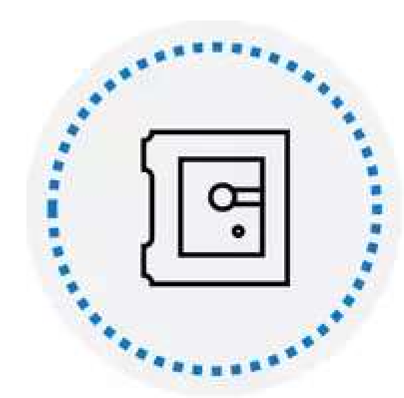


Dictionary attack

It is a type of identity attack.

A hacker attempts to steal an identity by trying a large number of known passwords.

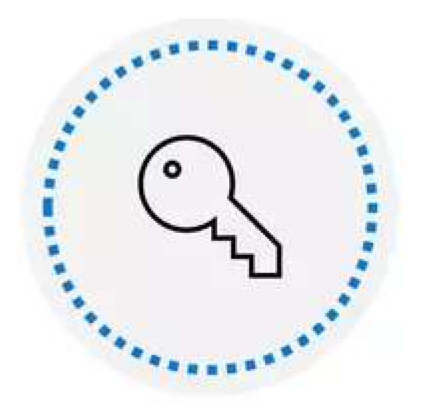
Dictionary attacks are also known as brute force attacks.



Ransomware

It is a type of malware that encrypts files and folders.

It attempts to extort money from victims.



Disruptive attacks

A Distributed Denial of Service (DDoS) attack attempts to exhaust an application's resources.

DDoS attacks can be targeted at any endpoint.

Other common threats include coin miners, rootkits, trojans, worms, and exploits and exploit kits.

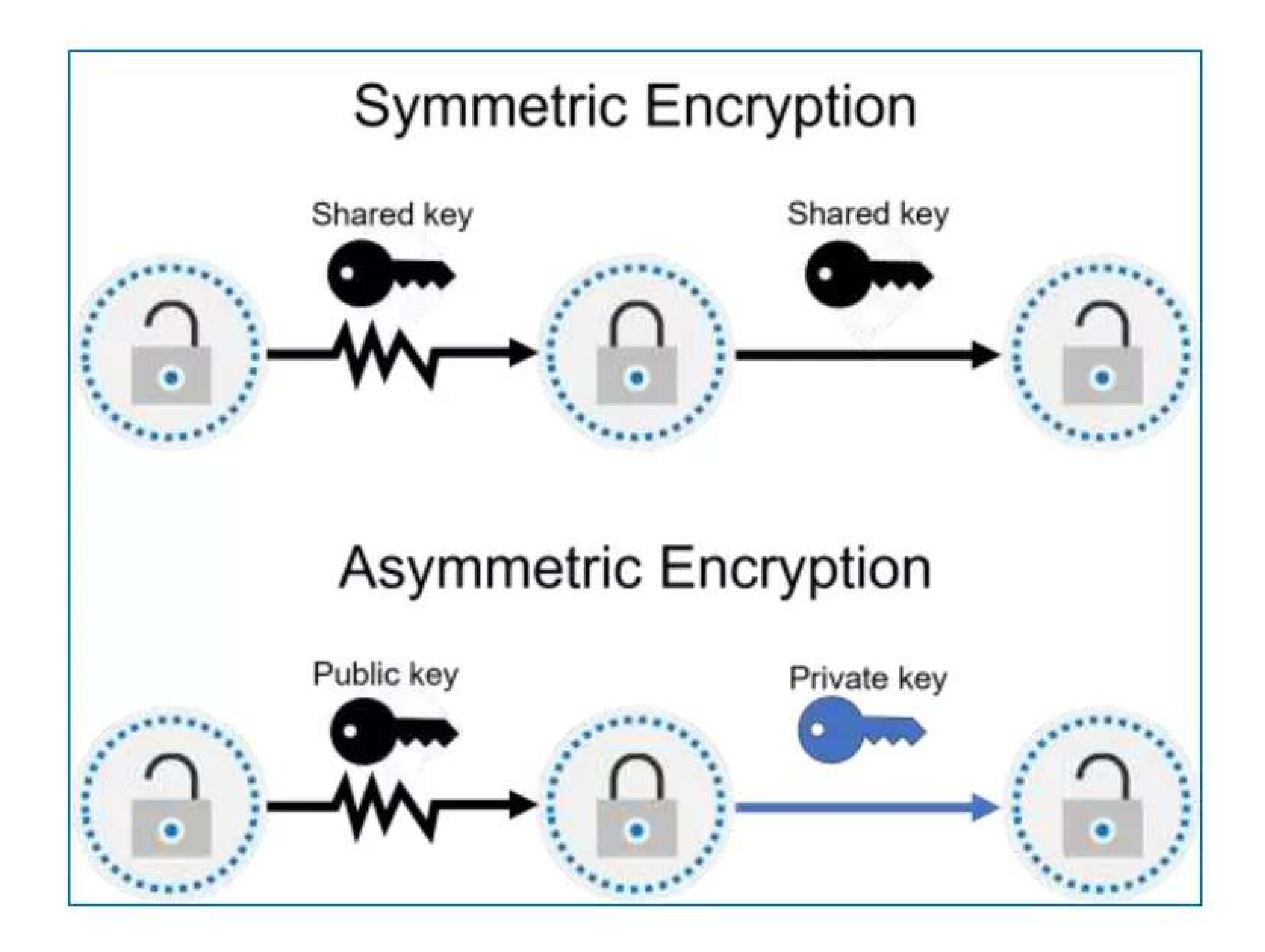
Encryption

Encryption is the process of making data unreadable and unusable to unauthorized viewers.

- Encryption of data at rest
- Encryption of data in transit

Two top-level types of encryption:

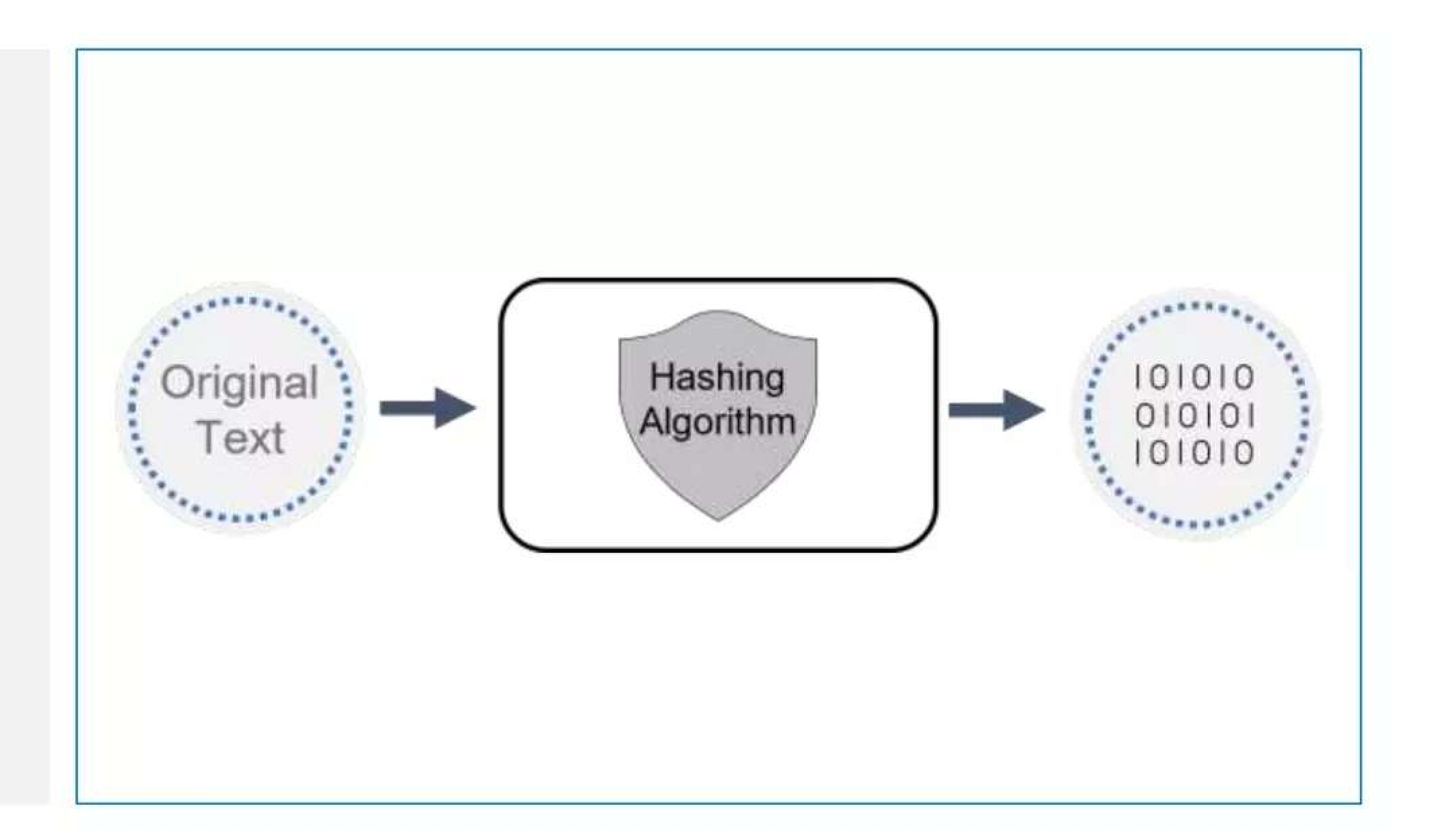
- Symmetric – uses same key to encrypt and decrypt data
- Asymmetric - uses a public key and private key pair



Hashing

Hashing uses an algorithm to convert the original text to a *unique* fixed-length hash value. Hash functions are:

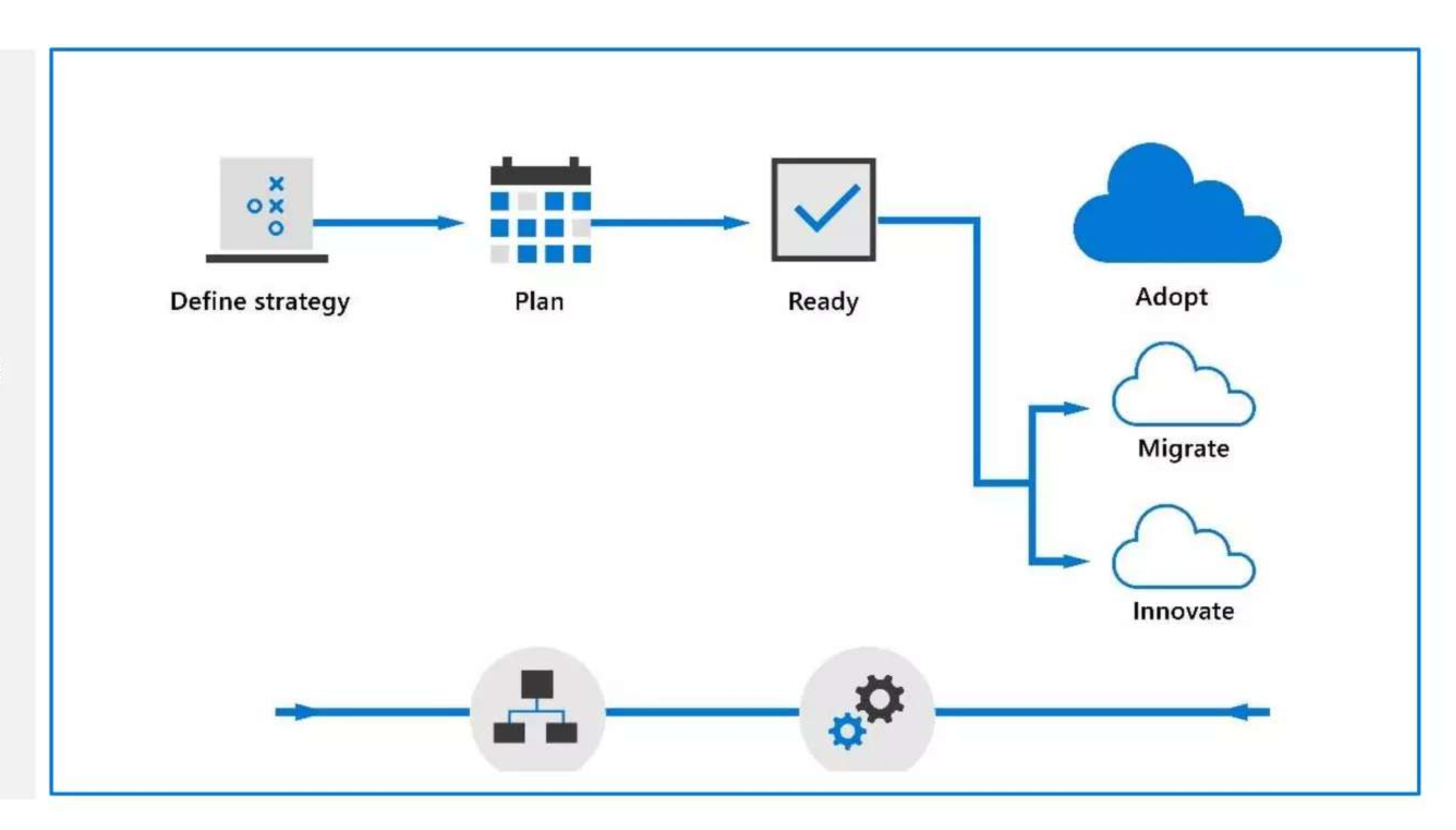
- Deterministic, the same input produces the same output.
- A unique identifier of its associated data.
- Different to encryption in that the hashed value isn't subsequently decrypted back to the original.
- Used to store passwords. The password is "salted" to mitigate risk of brute-force dictionary attack.



Microsoft Cloud Adoption Framework

Microsoft Cloud Adoption Framework

- Consists of documentation, implementation guidance, & best practices that support increased security and compliance
- Help businesses implement strategies necessary to succeed in the cloud.
- Lifecycle
    - Define strategy
    - Plan
    - Ready
    - Adopt (Migrate / Innovate)
    - Govern
    - Manage



Lesson 2: Describe identity concepts



Lesson 2 Introduction

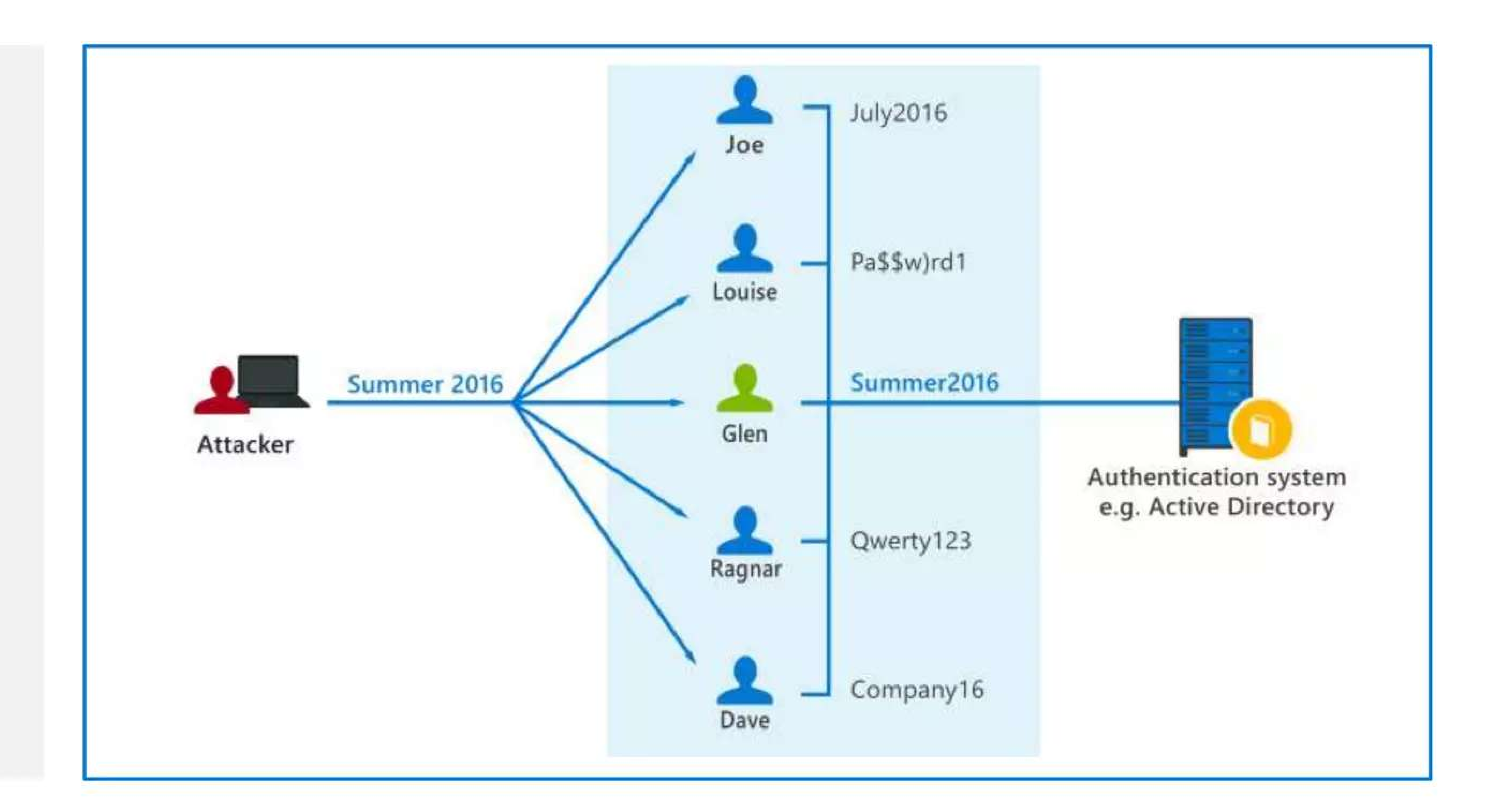
After completing this module, you'll be able to:

- Describe the concept of identity as a security perimeter
- Understand the difference between authentication and authorization
- Describe identity-related services

Common identity attacks

Types of security threats:

- Password-based attacks
- Phishing
- Spear phishing



Identity as the primary security perimeter

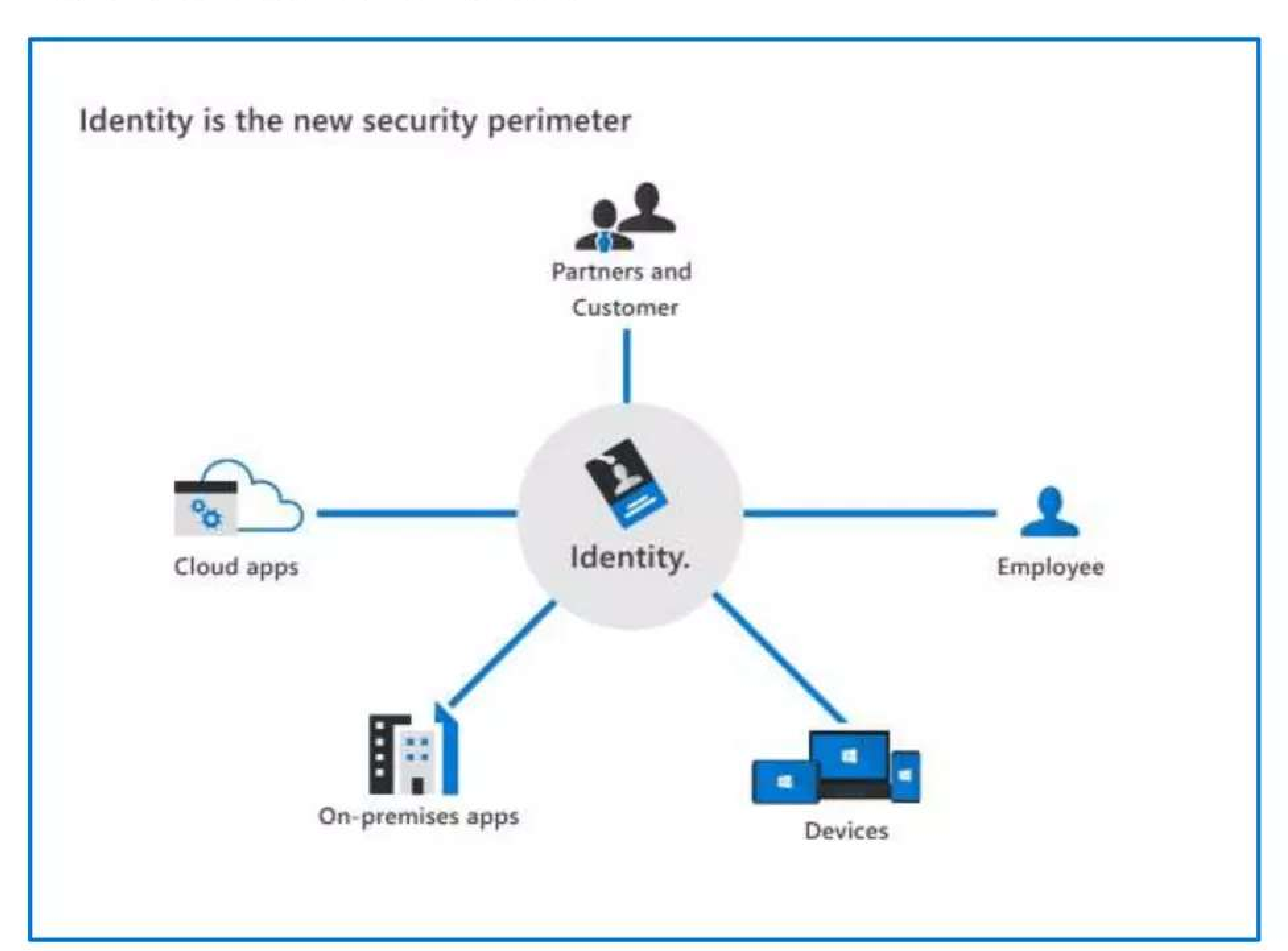
Identity has become the new security perimeter that enables organizations to secure their assets.

An identity is how someone or something can be verified and authenticated and may be associated with:

- User
- Application
- Device
- Other

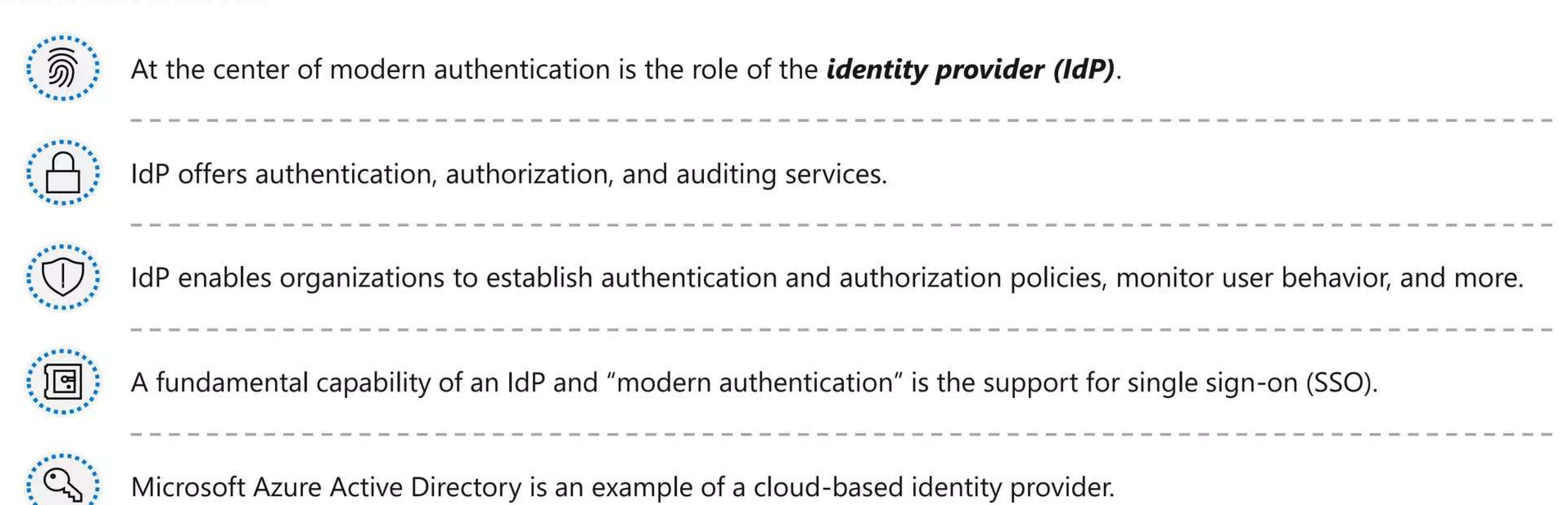
Four pillars of identity:

- Administration
- Authentication
- Authorization
- Auditing



Modern authentication and the role of the identity provider

Modern authentication is an umbrella term for authentication and authorization methods between a client and a server.



The concept of Federated Services

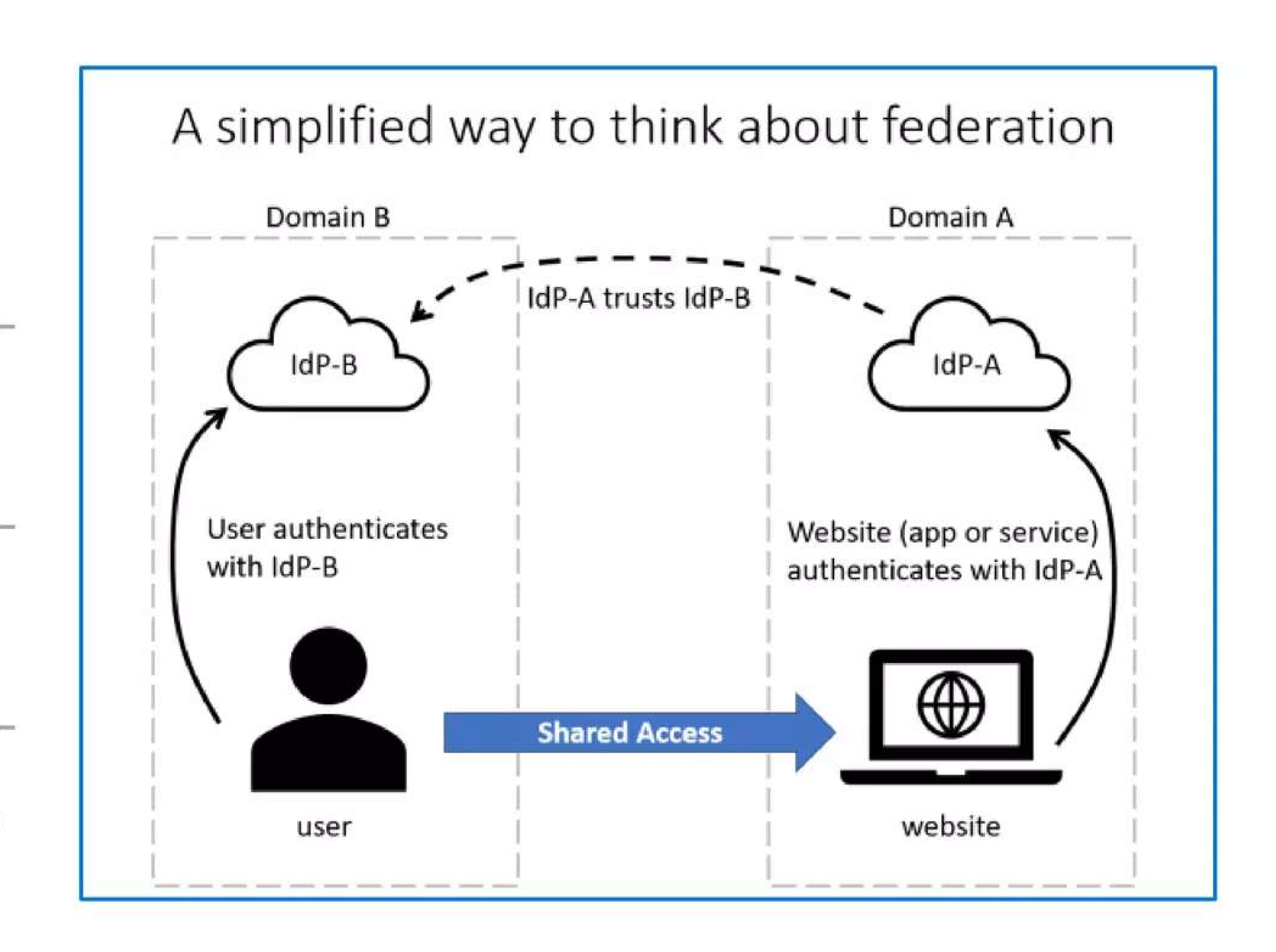
Simplification method of federation scenario:

The website uses the authentication services of IdP-A

The user authenticates with IdP-B

IdP-A has a trust relationship configured with IdP-B

When the user's credentials are passed to the website, the website trusts the user and allows access



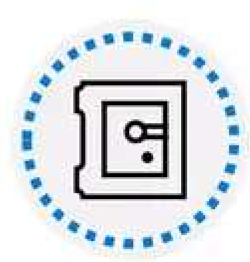
The concept of directory services and Active Directory



A directory is a hierarchical structure that stores information about objects on the network.



A directory service stores directory data and makes it available to network users, administrators, services, and applications.



The best-known service of this kind is Active Directory Domain Services (AD DS), a central component in organizations with on-premises IT infrastructure.



Azure Active Directory is the evolution of identity and access management solutions, providing organizations an Identity as a Service (IDaaS) solution for all their apps across cloud and on-premises.

Module Summary

In this module, you have:

- Learned about some important security concepts and methodologies.
  - Learned about the Zero Trust methodology, the guiding principles and the six foundational elements used in the Zero Trust model.
  - Looked at the shared responsibility model.
  - Learned about defense in depth and the tradeoffs associated with CIA triad.
  - Learned about common cybersecurity threats including threats to business and personal data.
- Learned about some important identity concepts.
  - Learned about the concept of identity as a security perimeter & the four pillars of identity
  - Learned about identity-related services, including the role of identity provider, federation, and directory services


Microsoft Security